NASA/TM-2008-215106

GN&C Engineering Best Practices For Human-Rated Spacecraft Systems

Cornelius J. Dennehy
NASA Goddard Space Flight Center, Greenbelt, Maryland

Kenneth Lebsock
Orbital Sciences Technical Services Division, Greenbelt, Maryland

John West
Charles Stark Draper Laboratory, Cambridge, Massachussetts

January 2008

The NASA STI Program Office . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the lead center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that complement the STI Program Office's diverse offerings include creating custom thesauri, building customized databases, organizing and publishing research results ... even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at ***http://www.sti.nasa.gov***

- E-mail your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA STI Help Desk at (301) 621-0134

- Phone the NASA STI Help Desk at (301) 621-0390

- Write to:
  NASA STI Help Desk
  NASA Center for AeroSpace Information
  7115 Standard Drive
  Hanover, MD 21076-1320

NASA/TM-2008-215106

GN&C Engineering Best Practices For Human-Rated Spacecraft System

Cornelius J. Dennehy
NASA Goddard Space Flight Center, Greenbelt, Maryland

Kenneth Lebsock
Orbital Sciences Technical Services Division, Greenbelt, Maryland

John West
Charles Stark Draper Laboratory, Cambridge, Massachussetts

NASA Engineering and Safety Center
Langley Research Center
Hampton, Virginia 23681-2199

January 2008

Available from:
NASA Center for AeroSpace Information (CASI)
7115 Standard Drive
Hanover, MD 21076-1320
(301) 621-0390

GN&C Engineering Best Practices For Human-Rated Spacecraft Systems

Cornelius J. Dennehy[1]
NASA Engineering and Safety Center (NESC), Goddard Space Flight Center, Greenbelt, MD 20771, USA

Dr. Kenneth Lebsock[2]
Orbital Sciences Technical Services Division, Greenbelt, MD, 20071, USA

John West[3]
Charles Stark Draper Laboratory, Cambridge, MA, 02139, USA

The NASA Engineering and Safety Center (NESC) recently completed an in-depth assessment to identify a comprehensive set of engineering considerations for the Design, Development, Test and Evaluation (DDT&E) of safe and reliable human-rated spacecraft systems. Reliability subject matter experts, discipline experts, and systems engineering experts were brought together to synthesize the current "best practices" both at the spacecraft system and subsystems levels. The objective of this paper is to summarize, for the larger Community of Practice, the initial set of Guidance, Navigation and Control (GN&C) engineering Best Practices as identified by this NESC assessment process.

I. Introduction

The NASA Engineering and Safety Center (NESC) is an independent technical resource that was formed in the wake of the Columbia tragedy to provide assessments of and recommendations to NASA programs on engineering and safety issues. A brief overview of the NESC organization along with a detailed portrayal of the operations of the NESC's GN&C Technical Discipline Team (TDT) is presented in Reference 1.

Recently the NESC completed an in-depth assessment to identify, define and document a comprehensive set of engineering considerations for the Design Development Test and Evaluation (DDT&E) of safe and reliable human-rated spacecraft systems. The Astronaut Office at NASA's Johnson Space Flight Center requested this NESC assessment. As part of this assessment NESC brought reliability subject matter, subsystem discipline, and systems engineering experts together to synthesize the current "Best Practices" that ensure robust, safe, and reliable critical human-rated spacecraft systems. The findings and recommendations resulting from this assessment are documented in Reference 2: Volume 1 of Reference 2 addresses the topic of spacecraft Systems Engineering for safety and reliability while Volume 2 of Reference 2 reports the subsystem-level findings and recommendations. The GN&C engineering Best Practices presented in this paper have been extracted and condensed from Section 7.5 of Volume 2 of Reference 2.

This paper will summarize the initial set of Guidance, Navigation and Control (GN&C) engineering Best Practices as identified by the NESC's GN&C TDT during this assessment process. These Best Practices address both the early and late phases of the overall DDT&E process. They cover a broad range from fundamental system architectural considerations to more specific aspects (e.g., mathematical modeling) of GN&C system design and development.

The motivation of this paper is to provide useful guidance, in the form of these Best Practices and other considerations and criteria, to the formulation, architecture, design, development and operation of GN&C systems for NASA's future human-rated spacecraft. It is sincerely hoped that engineers and managers can use this

---

[1] NASA Technical Fellow for GN&C, NASA Goddard Space Flight Center, Mail Code 590, Greenbelt, MD 20771, Member AIAA

[2] Senior Scientist, Orbital Sciences Technical Services Division, 7500 Greenway Center Dr. Greenbelt, MD 20770 Member AIAA.

[3] Program Manager, Space Systems Department, 555 Technology Square, Cambridge, MA, 02139, Member AIAA

information as an experience-based checklist that will increase design consistency, increase efficiency of the overall DDT&E effort, and most importantly, increase the confidence in the safety and reliability of the human-rated spacecraft's GN&C end product. A larger goal of this paper is to invite feedback on this initial set of Best Practices. These Best Practices are presented for review and comment by the larger GN&C engineering Community of Practice and the NESC GN&C TDT welcomes constructive comments on the information presented. Information from the Community on specific GN&C DDT&E Lessons Learned derived from both crewed and robotic flight system project experiences is sincerely solicited.

Multiple sources were used to uncover and gather GN&C relevant information for this NESC assessment. The GN&C TDT members who conducted this work performed an all-source search and capture process from which emerged a set of common recurring GN&C Lessons Learned and associated best practices. Lessons on robustness, reliability, and fault tolerance were extracted from a historical review of the Apollo, International Space Station and the Space Shuttle Programs. The historical GN&C record of both crewed and robotic missions was examined. Common GN&C mission success themes and elements were seen across human-rated and robotic spacecraft lines. The GN&C TDT found that the Lessons Learned from the large and diverse set of robotic spaceflight missions could contribute to the Best Practices for crewed space system GN&C engineering.

II. Motivation

There are many potential pitfalls that will threaten a successful GN&C system DDT&E process. Some of most common such pitfalls are listed below:

- ✓ Poor or Missing GN&C Requirements
- ✓ Failure to Stop Requirements Creep
- ✓ Poor Characterization of Mission Operational Regimes & Environments
- ✓ Inferior Architecture Development
- ✓ Unknown or Poorly Defined Interactions
- ✓ Unknown or Poorly Defined Interfaces
- ✓ Poorly Defined Coordinate Frames and System of Units
- ✓ Unknown and/or Incorrectly Modeled Dynamics
- ✓ Feedback Control System Instabilities due to Large Model Uncertainties
- ✓ Reliance on Any “Heritage”: in the Hardware, Software, Design Team, etc.
- ✓ Reliance on low Technology Readiness Level (TRL) GN&C technologies
- ✓ Sensor/Actuator Component Degradation & Failure
- ✓ Insufficient On-Board Processing Capability for GN&C Flight Software (FSW) Algorithms
- ✓ Inadequate Systems Engineering for Coordinated GN&C of Multiple Interacting Vehicles (e.g., during Rendezvous and Docking)
- ✓ Poor GN&C Fault Management Strategy
- ✓ Lack of Comprehensive Abort Strategy
- ✓ Inadequate “Safe Haven” capabilities
- ✓ Failure to “Design for Test”
- ✓ Failure to “Test as You Fly"
- ✓ Inadequate Hardware In The Loop (HITL) End-to-End Testing to Verify Proper Operations
- ✓ Inadequate Sensor-to-Actuator Polarity Tests (Lack of End-to-End Testing)
- ✓ Unresolved Test Anomalies & Discrepancies
- ✓ No truly independent Verification and Validation (V & V) process for GN&C

- ✓ Failure to “Fly as You Test”
- ✓ Failure to Have Crew and Operations Team “Train as You Fly"
- ✓ Inadequate Validation/Certification of GN&C Ground Data and Tools
- ✓ Insufficient Telemetry for GN&C Performance Monitoring and Anomaly Resolution During Launch, Early On-Orbit Checkout & All Mission Critical Events

It is highly unlikely that any single GN&C system development would typically fall victim to all, or even many, of the potential pitfalls listed above. An examination of the historical record does reveal however that several GN&C systems have been seriously victimized by one or more of the items listed above either during their design, development, test or operational phases. There are several points to be emphasized here. Spacecraft GN&C design and development mistakes are being repeated because key Lessons Learned from the past failures and mishaps are not being sufficiently infused into NASA's day-to-day GN&C engineering processes. It also appears that many previously established Lessons Learned must be relearned by the community.

The continued repetition of the same GN&C mistakes poses a risk to mission success that is potentially avoidable. GN&C engineers would be well served to keep this list of potential "what can go wrong" pitfalls in mind as they perform their daily job functions. Design reviewers could also use the list of potential pitfalls called out above as a top-level checklist to prompt inquiries into areas that have historically been problematic for GN&C system development. The NESC GN&C TDT believes the initial set of GN&C engineering Best Practices identified in this paper will proactively serve as a risk mitigating resource for GN&C engineers. If rigorously adhered to these GN&C Best Practices will help protect against the pitfalls cited above. One should clearly understand however that these Best Practices alone are not a substitute for the sound engineering judgment, experience and expertise, attention to day-to-day details and the broad intellectual curiosity needed by GN&C engineers to ensure mission success.

III. GN&C Engineering Best Practices

In the following pages of this paper the twenty-two individual GN&C System DDT&E Best Practices from Volume 2 of Reference 2 are each presented in a condensed one-page format. The authors encourage interested readers to obtain and review the original and complete version of each Best Practice, as documented in Reference 2, which contains an extended narrative as well as specific relevant linkages to a large set of real world mishap examples. In the following 22 pages, each Best Practice is first succinctly stated and then followed by a supporting technical discussion. Some of these discussions are illustrated with specific Lessons Learned from space mission failures and mishaps that occurred as a direct result of not observing the specific GN&C Best Practice. Lastly, a set of relevant questions is listed for each Best Practice identifying detailed areas for reviewers to probe.

IV. Summary

This paper has presented the initial set of the NESC GN&C TDT’s Best Practices for review and comment by the larger GN&C engineering Community of Practice. The NESC GN&C TDT welcomes constructive comments on the information presented.

The NESC GN&C TDT solicits further information from the Community on specific GN&C DDT&E Lessons Learned derived from both crewed and robotic flight system project experiences. Feedback commentary on the Best Practices presented herein and any new GN&C Best Practice information should be directed to the paper’s primary author. The GN&C TDT plans to maintain, distribute and periodically update, as comments and additional inputs are gathered, this initial set of GN&C Best Practices for broad general use by the GN&C Community of Practice.

GN&C Best Practice #1

Conduct a comprehensive and iterative GN&C subsystem architectural development activity very early in the DDT&E process.

The up-front "architecting-in" of robustness and reliability must be an integral part of the early steps of the GN&C Systems Engineering process. The selected architecture will directly influence the physical complexity, functional behavior, and performance of the GN&C subsystem, along with the related properties of safety, ease of implementation, operational complexity, affordability, robustness, serviceability, adaptability, flexibility, and scalability. A superior spacecraft GN&C architecture typically emerges from multiple iterations between the architects/designers and the stakeholder/customer/end user communities in which trades are performed between the mission requirements, operations concepts and resources constraints. Cost impacts (dollars, mass, power, etc.) should be understood for all GN&C requirements. "Tall pole" GN&C requirements should be clearly identified.

Desirable GN&C architectures allow for growth in the mission set and have high measures of effectiveness, safety, reliability, affordability, and sustainability. Inferior architectures may be "brittle" with few robustness qualities, overly complex (thereby masking adverse interactions and couplings), difficult to produce, test, operate, support, service, and upgrade. They are often prohibitively costly to adapt to evolving mission scenarios as the life-cycle extends beyond the anticipated time frame of the spacecraft's service life.

Parametric analyses, trade studies and error budgets should be used extensively to help guide the formulation of GN&C architectures and design concepts early in the DDT&E process. A lesson learned from the Apollo-era GN&C developers was the importance of early "hands-on" involvement by astronauts/crew in the formulation of the GN&C architecture. Early involvement and participation by system operators in GN&C system architectural decisions, and the subsequent design iterations, should return a significant payoff in safe and reliable mission operations over the spacecraft lifecycle.

Relevant Investigations:

1. Have the high-level mission objectives that drive GN&C design been defined, documented and clearly communicated? Same for subsystem-level functional, performance, and interface requirements that drive the GN&C architecture.
2. Have all the unique GN&C subsystem operational states/modes to be employed throughout the mission profile been identified?
3. Has the minimalist GN&C configuration that supports the mission objectives been defined as the starting point for architectural development?
4. Have the bounding environment, performance and reliability/fault tolerance requirements been determined for each GN&C mode?
5. Have multiple candidate GN&C architectures been defined and developed? What process, criteria, and measures of effectiveness were used to assess/evaluate competing architectures?
6. What is the conceptual basis and technical rationale for the overall GN&C architecture selected? Which particular GN&C requirements drove the selection of this architecture?
7. What process was used to select the type, size and number of the GN&C sensor and actuator hardware? How were the GN&C algorithms and flight/ground software elements selected?
8. Was the selection of the GN&C navigation and attitude sensor suite based upon performance requirements as well as the need for diversity of sensors in order to provide the capability to identify and eliminate faulty sensors?
9. Have all Single Point Failures (SPFs) in the GN&C architecture been identified and documented?
10. How will the crew interact with the GN&C?
11. Does the spacecraft GN&C architecture exploit hardware and software elements common to other spacecraft in the same product line?
12. What provisions in the selected architecture provide a "never give up" GN&C backup capability that keeps the crew safe if primary systems fail or become temporarily unavailable?
13. How sensitive/vulnerable is the GN&C architecture to faults, degradations, and failures in other spacecraft subsystems to which it is coupled and reliant upon?
14. Does the GN&C architecture compensate for the fact that GN&C components are subject not only to "hard" failure and malfunction, but also to degradation over the mission life?
15. Have the GN&C system architects utilized risk assessment techniques and reliability modeling to ensure the identification of all mission success and safety drivers? Is there a comprehensive understanding and awareness of risk likelihood versus risk consequence?

GN&C Best Practice #2

Search out, identify, and define all the interdisciplinary interactions and relationships that exist between the GN&C subsystem and other spacecraft subsystems.

An extremely important role of the GN&C Systems Engineer is the communication and coordination with other spacecraft subsystem leads. Neglecting, ignoring, over-simplifying, or overlooking the critical need for compatible design interactions between the GN&C subsystem and the other spacecraft subsystems can compromise the ability of the spacecraft to meet the desired requirements or can lead to mission mishaps and/or failures. The GN&C Systems Engineer needs to fully understand and appreciate the GN&C subsystem's relationship and interactions (in all forms) with the other spacecraft subsystems. Beware of complexity that can mask adverse interactions and couplings. All such relationships and interactions should be rigorously documented. Specific cases where the lack of full understanding and proper treatment of these relationships has led to failure or mishap include the TIMED and DART missions. The GN&C subsystem lead needs to fully define, through negotiations with other subsystem leads, and formally document the following:

- A summary description/schedule of those products that the GN&C subsystem lead needs to deliver to either the other spacecraft subsystem leads for their use in their subsystem-level design process or to the Spacecraft Systems Engineering lead. Those products may include GN&C trade study results, requirements documents, ICDs, error budgets, data/signal flow charts and block diagrams, work plans and schedules, technical memos, reliability analyses, fault trees, failure modes and effects analyses, test procedures, test reports, analytical procedures, analytical model interface requirements, analytical models, testbed and/or lab requirements, test article requirements, algorithm definitions, software builds, electrical harness diagrams, etc.
- A summary description/schedule of those products/documents the GN&C subsystem lead expects to receive from either the other subsystem leads or from the Spacecraft Systems Engineering lead to be used in the GN&C design process.

Relevant Investigations:

1. Have all the interfaces and interactions between the GN&C subsystem and all the other spacecraft subsystems been clearly defined and documented? For example, will the GN&C subsystem be responsible for controlling steerable/pointable spacecraft appendages such as communications antennas and solar arrays?
2. Have all the uncertainties and ambiguities, as well as the specific hardware/software faults, degradations, and failures, in other spacecraft subsystems that will affect the GN&C subsystem been identified? Has the potential impact of these been factored into the overall GN&C risk posture?
3. Have lists of GN&C products/documents, both deliverables and receivables, been generated? How were they developed? What technical interaction occurred to formulate these lists? How does one know the lists are comprehensive?
4. Are there formalized agreements/commitments in place between the individual subsystem leads (and between the subsystem leads and the Systems Engineering lead) to ensure the required products deliveries occur on time/within budget in both directions?
5. Have all the listed GN&C product deliveries been costed and budgeted by the Project?
6. Has the entire necessary GN&C infrastructure (i.e. computer-based analysis tools, engineering test unit hardware, testbeds, dynamic models, etc) been identified and costed and budgeted to support the generation and delivery of all the listed GN&C products?
7. Has an integrated schedule of all subsystem product deliverables and receivables been developed?
8. Has a product delivery critical path analysis been performed? Is the relative phasing of products acceptable? For example, will the necessary detailed mass properties information be delivered to the GN&C team in time to allow for sufficient stability and controllability performance analysis?
9. Are any GN&C subsystem product deliverables and receivables on the critical path? What steps have been taken to eliminate/mitigate schedule conflicts for the GN&C team?

GN&C Best Practice #3

Ensure a comprehensive set of Abort/Safe Haven strategies are formulated, and that Abort or Safe Haven functional capabilities are implemented, for all mission phases.

The GN&C system must operate not only under routine flight conditions but also must serve to ensure the safety of the crew under the extreme flight conditions when severe spacecraft (and launch vehicle) system degradations, malfunctions and failures occur.

An Abort strategy must be formulated to drive the actions to be taken to remove the spacecraft (with its crew) from an intolerably unsafe and possibly hazardous dynamic state. This unsafe condition could arise from many different problems that span the entire mission envelope. Aborts during launch and ascent will prematurely terminate the mission in order to return the crew safely to Earth. There could possibly be Abort scenarios where the mission is continued but with highly altered and much less ambitious objectives than were originally planned. In other cases, an Abort could result in the spacecraft being temporarily placed in a Safe Haven Mode.

Abort planning, including the definition of specific abort modes, is complex because of the myriad of potential mission contingencies that should be identified and evaluated. The Abort strategy will be constrained heavily by the GN&C architecture and conversely, as the requirements for certain Abort capabilities are refined through Systems Engineering analyses, they may drive changes to the existing GN&C design and capabilities. Abort planning should cover a wide range of potential system degradation, malfunctions, and failures. Anomalous conditions such as launch vehicle engine failures, engine under-performance, propellant tank leakage, crew cabin pressure leakage, loss of electrical power, loss of vehicle cooling, etc. are typically considered when doing Abort planning. A detailed risk assessment analysis should be used to guide this Abort planning. Abort planning will first consider those phases of the mission where risk levels are the highest and where the time-constants of the system dynamics are so short (relative to human detection/reaction times) that extensive on-board human intervention by the crew is precluded.

Good spacecraft engineering practice would dictate consideration of a Safe Haven attitude control mode to be entered in spacecraft emergencies. Its primary purpose is to stabilize the spacecraft by damping angular rates to within pre-set limits. A secondary purpose is to control the attitude of the spacecraft in a power-safe and thermal-safe orientation that allows communications with the ground operations to be re-established.

The Safe Haven mode should behave very predictably while minimizing its demands on the rest of the spacecraft to facilitate spacecraft survival, diagnosis, and recovery. For example, as the NEAR spacecraft approached rendezvous with the asteroid EROS it had a propulsion system anomaly that caused loss of contact within 37 seconds. Since the round-trip light time was nearly 40 minutes, it was critical that the ACS could operate autonomously in Sun Safe mode for the next 27 hours until communication was restored. The GN&C equipment used to implement this Safe Haven function should be as separate and independent as possible from the equipment used by the primary spacecraft attitude control system. The Safe Haven mode design must take into account the spacecraft thermal design, mechanical design (including array orientation and mass properties), and attitude control electronics design. Safe Haven is driven by the GN&C subsystem but clearly is a spacecraft System-level issue.

Relevant Investigations:

1. What are the abort strategies for the various phases of the mission?
2. Are passive abort schemes employed wherever feasible, especially during rendezvous?
3. Are Abort scenarios and the Safe Haven modes detailed in the Mission Concept of Operations and the GN&C Requirements documents?
4. Does the Safe Haven mode(s) autonomously activate? Can the crew command it if necessary?
5. Is the Safe Haven mode simple and employ the minimum hardware set required to maintain a safe spacecraft attitude?
6. How long can the spacecraft operate in the Safe Haven mode without crew or ground interaction?
7. Will the GN&C recovery from a Loss of Control or a Lost in Space condition require support from either the crew or the ground or will the GN&C recover autonomously from a cold-start?
8. Can a single credible fault both trigger Safe Haven entry and cause Safe Haven failure?
9. What Safe Haven attitudes are acceptable for thermal, power, and communications safety and can those attitudes be stabilized passively?
10. Have Safe Haven recovery procedures been validated during mission simulations?
11. Has a rigorous risk assessment been performed to support a Project-level decision as to whether or not to perform an on-orbit Safe Haven test?

GN&C Best Practice #4

Host mission critical GN&C flight software processing functions on a spacecraft processor with sufficient computational power and assign sufficient processing priority to execute at the necessary frequency that has been established by analysis.

In virtually all spacecraft, the reliable realtime execution of GN&C flight software on a digital flight computer is an absolute requirement for mission success. In most applications, the GN&C sensor measurement data are acquired and processed on a cyclical basis. These sensor-processing algorithms are mode-dependent and are used to compute the spacecraft's dynamic state. Sensor data is processed by controller algorithms to compute actuator commands, which are then output cyclically to force and torque producing devices. In addition, GN&C Fault Detection, Isolation and Recovery (FDIR) processing must be performed as well as the GN&C command/telemetry processing functions. All these GN&C realtime software tasks must be scheduled and performed flawlessly at the prescribed cyclic frequencies that have been established by analysis for each mode of operation.

A digital computer, along with its realtime operating system, must be carefully selected by the GN&C developer to adequately perform the scheduling and execution of GN&C processing tasks in such a way that the demanding flight safety critical timing requirements are reliably met with margin. Flight safety critical "hard realtime" processing systems, such as a spacecraft's GN&C system, are different from other processing systems because a failure to satisfy timing requirements may have unacceptable consequences for the mission. These hard realtime systems operate in an environment that has stringent safety and response time constraints.

The result of missing a deadline imposed on a GN&C task execution may be catastrophic. For this reason, there should be a great emphasis early in the design stage on the selection of a digital computer, and its RealTime Operating System (RTOS), that can satisfy GN&C processing requirements with demonstrable margin. A relevant example of this occurred during powered descent of the Apollo 11 LM when a guidance computer problem occurred which threatened the success of the landing. A previously encountered, but uncorrected problem in the Apollo 11 LM's rendezvous radar's computer interface stole approximately 13% of the computer's duty cycle resulting in five program alarms and software restarts. The guidance computer had become overloaded and it had more work to perform than processing capability.

Relevant Investigations:

1. What is the basis for GN&C FSW code, data, and throughput requirements?
2. How were the GN&C computational power and processing priority requirements established and how will they be verified?
3. What is the rationale for selection of the flight computer that will perform the GN&C flight software processing (i.e. performance, heritage, RTOS, etc.)?
4. Do the avionic elements for data transfer, satisfy the GN&C sensor sampling and actuator commanding rate and data latency requirements under nominal and stressed conditions?
5. Does the GN&C subsystem developer have familiarity with the flight computer hardware, its RTOS, as well as the associated software development and test tools?
6. What are the current estimated margins for GN&C code, data, and throughput? What are these margins predicted to be at PDR, CDR, PER, and at launch?
7. What are the minimum acceptable thresholds for GN&C code, data, and throughput margins?
8. What risk mitigation plans are there to ensure that margins are attained?
9. What corrective action strategies will be used when GN&C flight software margins deviate from the plan?
10. Will GN&C flight software processing functions be performed on a single dedicated GN&C computer, on multiple dedicated GN&C computers, or on shared general-purpose spacecraft computers? Are dissimilar computers used for GN&C processing?
11. If the computer is shared, how are the worst case requirements/interactions for the other processes emulated or simulated during test?
12. Have worst case execution times of each GN&C mode processing been determined via test?
13. What are the on-orbit GN&C FSW maintenance plans and procedures?
14. Will there be a dedicated testbed facility for on-orbit FSW maintenance and support functions?
15. What is the capability to implement on-orbit code patches?

GN&C Best Practice #5

Ensure that autonomous GN&C fault management is be independent of all hardware and software that might be involved in either causing or diagnosing a fault.

The spacecraft should have an independent Safe Haven attitude control mode to be entered in spacecraft emergencies. Safe Haven Mode should behave very predictably using components that are completely independent of those used to diagnose the fault. The same sensor (e.g. a gyro) cannot be relied upon to monitor the performance of a control loop if it is also used as an element of that control loop. Correct diagnosis is more certain when a diverse set of dissimilar hardware and/or software is used to perform FDIR.

The fault management system (particularly the software) can be a source of single-point failures. Inaccurate situational awareness can lead to wrong disposition. Faulty sensor data may create a phantom problem and spoof the fault management system into taking precipitous actions such as resets. Resets must be managed with care to avoid the possibility of becoming trapped in an endless cycle of resets. In addition, a reset during anomalous conditions may reset relays into a dangerous state. Fault protection must take proper action regardless of spacecraft state.

If a fault is detected that may have been caused by a control actuator, then that actuator should be disabled and a functionally redundant actuator substituted for it. For example, if the reaction wheels fail to control attitude then a backup set of thrusters might be used in their place. Special care must be exercised if a fault is detected during thrusting operations. Any thrusters that may have been involved in causing the fault must be disabled.

Both the Clementine and NEAR spacecraft had long sequences of improper thruster commands from their flight computers while out of contact with the ground. After mapping the Moon, Clementine was injected into an Earth swingby orbit to continue its mission with a planned flyby of a near-Earth asteroid. The on-board software crashed which caused telemetry to freeze and the computer to erroneously fire ACS thrusters for 11 minutes. A "watchdog timer" algorithm, designed to stop the thrusters from continuously firing, could not execute because the computer had crashed. Clementine was left spinning at 80 rpm with no ACS fuel left to despin, thus ending its mission.

The Near Earth Asteroid Rendezvous (NEAR) mission decided, partly due to Clementine's experience, to use a different burn philosophy: 1) There would be no burns with critical timing and 2) If an anomaly was detected during a burn it was better to shutdown, correct the problem if any, and try again. The mission plan provided a second opportunity to achieve a capture orbit at the asteroid. The watchdog function was hardwired in case the computer shut down. These were wise decisions because as NEAR started to rendezvous with its asteroid, the main engine burn aborted within a fraction of a second after bi-propellant initiation due to on-board software limits being exceeded. The S/C signal was lost 37 seconds following abort and the attitude control system operated autonomously for the next 27 hours, until communication were restored and the computer could be rebooted. During that time, NEAR's thrusters fired thousands of times, but each firing lasted only a fraction of a second before being cut off by the still-operative watchdog timer. Subsequently, given a second rendezvous opportunity, NEAR entered orbit around the asteroid Eros and successfully completed its mission.

Relevant Investigations:

1. Can a single credible fault (e.g. a failed gyro) both trigger Safe Haven entry and then cause Safe Haven failure?
2. In the event of a fault, will the spacecraft autonomous management system and the ground controller be provided with correct information?
3. Does Safe Haven require ground intervention?
4. Can a momentary wiring short in the bus reset all relays into an undesired configuration?
5. Is the system designed to revert to "last known good state"? Are there system elements that can "fail silent"?
6. Does the fault management design consider all operational possibilities such as solar array mispointing, engine abort, or eclipse transient?
7. Will the fault correction software execute if there is a major anomaly such as a computer freeze?
8. Will the fault management system be tested on the flight spacecraft before launch?
9. Is the fault management system enabled only in those mission phases where it serves a useful purpose?
10. What are the safety positive interlocks in the architecture for inhibiting thruster firings during prescribed "no fire" periods (e.g., during EVAs or during fault diagnosis periods)?
11. What are the system requirements and design drivers that establish the time constraints on entry into Safe Haven and the maximum time period that Safe Haven can be maintained?

GN&C Best Practice #6

Ensure that adequate Systems Engineering establishes, and properly flows down, the higher-level of GN&C requirements necessary for a multi-vehicle system of spacecraft that must safely interact during the Rendezvous, Proximity Operations, Docking, and Undocking (RPODU), as well as mated, operational phases of the mission.

The hardware and software implementation of a RPODU capability must be seamlessly architected, integrated, and coordinated between two or more interacting spacecraft GN&C subsystems. The requirements for the individual spacecraft GN&C systems should flow down from the overriding requirements for the coordinated guidance, navigation, and control of the interacting spacecraft.

The requirements, components, algorithms, operational methods and fundamental dynamics of the RPODU and the mated operational phases of the mission must be carefully factored into the GN&C architecture as early as possible in the DDT&E process. This is necessary to avoid potential operational complexity, inefficient use of ground and/or space resources, spacecraft collisions while docking or undocking, control system interactions, loss of control authority, and/or dynamic instabilities of mated spacecraft configurations. Due to different inertia properties, control system bandwidth, and pointing requirements following rendezvous and docking the control authority required for the mated configuration may not be compatible with that provided by the individual spacecraft. Flexibility effects on stability may become the dominant design driver if actuators and/or sensors that are located on different spacecraft modules are used to control the mated system.

The Demonstration of Autonomous Rendezvous Technology (DART) mission was to demonstrate that a pre-programmed and unaided spacecraft could independently rendezvous with a non-maneuvering and cooperating satellite (Reference 3). DART performed as planned during the early phases of its mission. During proximity operations, however, the spacecraft began using much more propellant than expected. Before its propellant supply was depleted, it began a series of maneuvers for departure and retirement. DART had actually collided with the target spacecraft a few minutes before initiating retirement. The DART Mishap Investigation Board (MIB) determined that there was an inadequate Systems Engineering process which failed to reveal a number of design issues contributing to the mishap. In some cases, there was insufficient system-level understanding of the potential effects of complete or partial loss of functionality. Performance requirements for critical capabilities, such as collision avoidance, were not detailed enough. Having adequate Systems Engineering is a critical lesson learned from the mishap that will help enable the future development of RPODU capabilities.

Relevant Investigations:

1. Is the rendezvous trajectory passively safe so that collision avoidance is intrinsic in the event of a sensor, computer, or thruster failure?
2. Does the closing trajectory accommodate dispersions in range, range rate, and cross track? What is the sensitivity of consumable allocation and the timeline for rendezvous and docking to variations in the dispersions?
3. Is there a seamless transition between autonomous and astronaut control during rendezvous, docking, and proximity operations?
4. Does the GN&C mechanization accommodate astronaut commands that are intuitively based on the human perception of LOS data?
5. How will the individual spacecraft GN&C subsystems interface and interact with each other when mated in a stack?
6. Does the spacecraft GN&C architecture require the inclusion of command, data, and telemetry interfaces to allow the use of GN&C sensors and actuators on different modules while mated?
7. How well will the rigid body mass properties and modal frequencies of the stacked configurations be known in advance and how sensitive is the GN&C system to parameter variations?
8. How adaptive is the GN&C attitude/momentum control system? Is there a provision for a composite (i.e., stacked module configuration) mass properties estimator?
9. Has an analysis of degraded rendezvous sensor functionality and maximum design condition variations been performed and not just an evaluation of complete loss of sensor functionality?
10. Has a minimum fault tolerance level been established for the rendezvous vehicles?
11. Is an independent collision avoidance sensor employed on the rendezvous spacecraft?
12. Do the specifications for the rendezvous spacecraft contain detailed fault detection, isolation, and recovery requirements?

GN&C Best Practice #7

Critically evaluate redundancy with identical GN&C hardware components to ensure that the net effect is an overall increase, rather than a decrease, in system reliability. Always keep in mind that redundancy inherently adds complexity.

Hardware redundancy is used to tolerate hardware failures. However, redundancy is not always desirable in terms of GN&C fault management. If the primary and redundant units share the same current feed, software, or processor, one flaw in the primary component can cause the backup to fail in the same way. A redundant GN&C configuration using unproven components is not a solution. Examples include the experience with the HEAO spacecraft 6-gyro configuration that experienced failure of all six gyros and the Hubble Space Telescope that required several on-orbit gyro package replacements.

Only design diversity can mitigate design errors. Diversity uses redundant, dissimilar hardware and/or software and a method to establish which is working correctly. Hardware redundancy does not necessarily protect against software faults. Redundancy of function by a different implementation may provide safer fault management than redundancy with identical implementation.

When designing redundancies into systems, consider the use of non-identical approaches for backup, alternate, or redundant items to protect against the potential pitfall of common cause failures. A fundamental design deficiency can exist in both the prime and backup system if they are identical. For example, the rate gyros in the Skylab attitude control system were completely redundant systems, i.e., six rate gyros were available, two in each axis. However, the heater elements on all gyros were identical and had the same failure mode. Thus, there was no true redundancy and a separate set of gyros had to be sent up on Skylab 4 for an in-flight replacement.

The maiden flight of the Ariane 5 launcher on June 4, 1996 relied on identical GN&C hardware and software for redundancy. Unfortunately at about 39 seconds into the flight the primary Inertial Reference Unit (SRI-1) stopped sending correct attitude data to the On-Board Computer (OBC) due to a software exception. The OBC switched to the backup inertial unit, but SRI-2 also failed due to its independently determined software exception. The OBC could not switch back to SRI-1 so it took data that was actually part of a diagnostic message written to the data bus by SRI-2. This data was wrongly interpreted as flight data and used for Thrust Vector Control computations. The sudden gimballing of both solid booster nozzles and the Vulcain main engine, up to their physical limits, caused the angle of attack to increase sharply giving rise to intense aerodynamic loads leading to destruction of the vehicle.

A fundamental fault in using identical redundant systems containing both hardware and software is that software failure modes are quite different from those of hardware components. Hardware components are never perfectly identical and even slight differences will result in apparently random failures. Software failures are systematic because identical software is truly identical. The failure of the Skylab gyros was not immediately catastrophic because even though they had the same failure mechanism they failed at different times and humans had time to replace them. The failure of the Ariane Inertial Reference Units was immediately catastrophic because both systems failed simultaneously due to identical software.

Relevant Investigations:

1. Has the use of diverse GN&C components, to provide functional redundancy in the architecture, been traded against the resources that will be needed to source/procure, qualify, test and integrate these additional components?
2. Does the use of diverse GN&C components, to provide functional redundancy, degrade performance? Is the degradation acceptable?
3. Does switching between redundant units ensure a safe transfer for all credible failure paths (e.g. parts failure, start-up transients, latch-up, over voltage, and EMI, software endless looping)?
4. Have the GN&C system architects paid sufficient attention to common cause and common mode failures that may defeat the intended reliability and/or safety improvements of including redundant components?
5. Have the GN&C system architects performed a top-down assessment of potential failure modes and the associated impact on system reliability and safety?
6. Is the backup software identical or was it independently developed and tested to provide functional equivalence?

GN&C Best Practice #8

Evaluate all heritage hardware and software elements in the GN&C architecture in light of potential differences in build, flight configuration, mission application, flight environment, and design/operations teams. Be extremely cautious about qualifying flight hardware or software by similarity.

Heritage equipment fielded in a robotic orbital spacecraft mission or an aircraft application may not be applicable for use in a crewed vehicle, especially one envisioned for a Lunar or Mars venture. The capabilities may not be consistent with the flight requirements and operational modes. Any operating environment differences are likely to have serious implications. Their implementation in a Fail-Operational architecture may not be possible or may be complex with vulnerabilities.

There have been three noteworthy examples of this on the Shuttle Orbiter: inertial systems, GPS receivers, and processors. The original selection of the Shuttle Orbiter's inertial system was derived from the heritage experience of the KT-70 system fielded in tactical aircraft applications. Incompatibilities in equipment capabilities and environmental provisioning required extensive redesign resulting in essentially a customized configuration called "HAINS" for High Accuracy Inertial Navigation System. The selection of a tactical aircraft GPS receiver was inconsistent with space environment conditions and software limits on the velocity range and codes, etc.. These issues were only realized after commitment to this component. The initial selection of the Shuttle computer based on the tactical aircraft "4-Pi Processor" resulted in initial reliability problems and limitations in the fault tolerant implementation. Reliability and memory limitations led to an upgrade to an AP101S processor in later Shuttle usage.

Changes introduced to meet performance operational requirements have to be fully validated to assure that reliability objectives are met. Before committing to a lower cost heritage unit sufficient analysis and test is required to verify suitability in the new mission application. Any change in the application of previously developed hardware, software, or operational procedures may require a certain amount of redesign to ensure proper functionality in the new circumstances. For example, fault management circuits may need to be redesigned because when a heritage unit is scaled up, key parameters such as start-up current and rise time may change. Some changes may require complete re-qualification of the heritage component or process. Design upgrades made while an old unit sat on the shelf should be considered if an old unit is being re-commissioned for flight. It is not sufficient for the replacement parts or units to merely meet lot acceptance specifications. Component qualification must be based on sufficient engineering data. That a few items worked is not sufficient—statistical data may be required to show margin of safety.

Software reuse should be thoroughly analyzed to ensure suitability in a new environment, and all associated documentation, especially assumptions, should be reexamined. Removal of obsolete portions of the code should be considered if legacy software is being reused. Extensive testing, including software loop and path testing, should be performed at every level, from unit through system test, using realistic operational and exception scenarios. The software exception that caused the inertial reference units on Ariane 5 Flight 501 to stop supplying valid attitude data was caused by the reuse of unnecessary software from Ariane 4. The Ariane 5 trajectory was sufficiently different to cause an Operand Error when horizontal velocity exceeded the range of values for Ariane 4. The software had not been designed or tested for use with the Ariane 5 trajectory.

Relevant Investigations:

1. Has a Heritage Review been conducted to assess and document how the requirements, environments, lifetime of the present mission, compare to capability of the heritage hardware and software?
2. Have all "heritage equipment" test and flight anomalies been resolved?
3. Have catastrophic failures that involved similar technologies been reviewed?
4. Have replacement materials and parts that are used in "heritage equipment" been fully qualified?
5. Is the heritage hardware being assembled in exactly the same manner as the original or is it being built to print by some other process that may not be the equivalent of the original?
6. What is the requalification plan and process if the original hardware or software is being reused?
7. Under anomalous circumstances, is it possible for obsolete segments of legacy code to be executed?
8. Has the "heritage" of the unit being considered been analyzed for relevancy to the current mission application, especially in terms of the operating environment, parts, life, and other intrinsic characteristics?

GN&C Best Practice #9

Make certain that new GN&C technology is well qualified. It must have sufficient statistics to show an acceptable safety margin and flight proven alternatives must be identified.

Emerging GN&C technology has the potential to allow space missions to be performed more affordably, more safely, more reliably, more effectively and in new operational regimes. This technology promises either to provide GN&C performance previously unattainable, or to provide the same level of performance with fewer resources than previously required.

Currently there are multiple GN&C related items in the in technology pipeline (e.g., MEMS inertial sensors) at various level of Technology Readiness Level (TRL) maturity. However, there are very limited flight opportunities for any of these GN&C technologies to be validated on-orbit. It can be assumed that any technology assessed to be at a state less than TRL 7 (Prototype Demonstrated in Space Environment) will require significant funding and schedule resources to attain "flight qualified" status. Inclusion of emerging GN&C technologies (any item objectively evaluated to have a TRL less than 7) should be carefully considered, justified with a strong engineering rationale for its infusion, and carefully planned.

An example of this in the GN&C arena was the premature adoption in the mid-to-late 1980's time period of Ring Laser Gyro (RLG) technology as a substitute for the traditional spinning mass "iron" mechanical gyroscopes in some spacecraft attitude determination and control applications. The transition of the RLG technology was based upon the favorable insertion and performance of the RLG technology in inertial navigation systems for terrestrial, airborne and marine military platforms. The point is that when first infused into NASA space missions the RLGs were a non-space qualified technology. RLGs had not attained TRL 7 (i.e., prototype demonstration in an operational environment) in the space environment although it was in broad operational use (TRL 9) in the aforementioned terrestrial, airborne and marine applications. In retrospect life tests and better qualification may have prevented numerous on-orbit anomalies and failures with this RLG technology.

Relevant Investigations:

1. What GN&C technologies, with TRL less than 7, have been considered for the mission and why?
2. What technology cost/benefit trades have been performed?
3. What specific GN&C technologies are incorporated in the baseline architecture and what is the engineering rationale for their inclusion?
4. Is the GN&C architecture such that one new technology relies on another new technology in order to achieve the desired flight performance?
5. What is the GN&C Technology Development Plan?
6. What is current TRL of each GN&C technology? What TRL is needed at PDR, and at CDR?
7. Have technology readiness gates and objective criteria been formulated to meaningfully assess technology advancement?
8. What is the spacecraft prime contractor's level of familiarity with each selected GN&C technology?
9. Was the technology developed "in-house" by the spacecraft prime contractor? If not, what is the relationship (technical and business) between the prime contractor and the GN&C technology provider?
10. How is the GN&C technology development being funded? Are contractor IR&D funds being used or is another government or commercial project funding the development, or it is being funded by the project directly? How much control does the project have over the funding, and what risk funding has been planned?
11. Does the GN&C implementation plan include provisions for pre-planned higher-TRL (or ideally, flight proven) alternatives to mitigate risk that baselined low-TRL technologies don't mature consistent with the Project schedule?
12. Have both the GN&C subsystem-level and the spacecraft system-impacts of reverting to these flight–proven alternatives been assessed?
13. Are all technology test facilities in-house?
14. When prescribed GN&C technology readiness gates are not met, is the Project prepared to cease development and implement preplanned alternatives?
15. What are the qualification criteria for all new technologies?

GN&C Best Practice #10

"Design for Test": Consider the degree of difficulty of performing ground validation testing and pre-flight calibration when evaluating candidate GN&C subsystem architectures.

Design for test and the adequacy of the test capabilities often is an afterthought in design. Involvement of the test engineers in the design process enables definition of needed data interfaces and readouts that evidence both satisfactory operation and trending as well as failure isolation and often failure prediction capabilities. Early definition of test requirements provides a sound basis for test facility development and timely equipment readiness.

Making design provisions for test as an afterthought leaves uncertainties in function and increases the difficulty of isolating a failure mechanism in an integrated system. Special one-of-a-kind test configurations (e.g., break out boxes and digital waveform analyzers) implemented during the validation testing phases may allow extensive data access but cannot (and should not) be carried forward in the full-up system flight configuration. Similarly an over-emphasis of the hardware test point concept is difficult to be realized in a flight configuration and may be undesirable. The Block I Apollo GN&C hardware configuration implemented extensive test point connectors in the hardware elements and was only consistent with an ad-hoc debugging process, which introduced possible failure modes. This cumbersome and risky method was abandoned in the Block II flight hardware. Instead, Block II relied on availability of a telemetry data stream and key performance indicators. In this improved Block II design, sufficient data was therefore made available and was safely buffered to support testing activities.

In summary, test planning and implementation consistent with the use of the flight system's telemetry downlink is most desirable for supporting both ground pre-launch checkout testing and flight operations. Spacecraft telemetry systems should be designed to be configurable for high-rate "every cycle" GN&C data capture and output for use in ground test verification and troubleshooting.

Relevant Investigations:

1. Is there a plan for early definition of GN&C test requirements and the identification of required GN&C test facilities? Will this work be done concurrently with the early GN&C system design effort?
2. Is there evidence that GN&C test engineers are adequately integrated into the GN&C design process to enable definition of needed data interfaces and readouts that will indicate both satisfactory subsystem operation and trending as well as failure isolation?
3. Has the use of existing special purpose GN&C test facilities and equipment been shown to be adequate, operational, and available?
4. What are the plans, schedule and resources to upgrade, retrofit, and re-calibrate the existing GN&C test facilities and equipment?
5. What is the basis and rationale for new test facility development?
6. What are the plans, schedule, and resources to develop new GN&C test facilities and equipment?
7. What evidence is there that the proper planning has been done to ensure timely test equipment readiness?
8. Have all non-flight GN&C Special Test Equipment (STE), test fixtures and associated Ground Support Equipment (GSE) needs and requirements been identified?
9. What efforts are being made to minimize the needs for non-flight GN&C STE, test fixtures and associated GSE?
10. What GN&C testing can be performed at the fully integrated spacecraft level prior to shipment to the launch site? What are the specific limitations to GN&C testing at this point in the spacecraft development?
11. What GN&C testing can be performed at the launch processing facility? What are the specific limitations to GN&C testing at this point in the spacecraft pre-launch processing?
12. If the fully tested and flight-ready GN&C subsystem hardware/software configuration is altered, what are the requirements and the planned approach for re-test?
13. Can the test data gathered at the component level, subsystem level, and system level be integrated into a common performance trending database?

GN&C Best Practice #11

Define and document the coordinate frames and the system of units (and associated conversion factors) that are to be employed and rigorously enforce compliance.

The use of a common set of units and coordinate frames is necessary to prevent miscommunication of technical information. The result of miscommunication can vary in severity -- from a delay in schedule to resolve any discrepancies, to the cost of reworking ACS components, or to (in the extreme) un-recoverable mission failures due to ACS design errors.

Two systems of units are in common usage on US space programs: metric and English. Individual groups, even within the same company, may use different systems of units because they normally support different customers. The project level systems engineer is responsible for specifying a consistent set of units that will be used throughout the project. The Project Systems Engineer may permit a parameter to also be expressed in a second set of units inserted parenthetically after the standard units, if doing so will improve understanding.

Similarly, a great number of coordinate reference frames are used in the development of space systems. Different disciplines will naturally use different reference frames for detailed analyses of orbit mechanics, attitude control, launch loads etc. Each of the discipline reference frames must have a clearly defined origin of coordinates and orientation with respect to an established standard.

It is sound engineering practice to generate and maintain a Project-controlled document that captures the following GN&C items:

- The system of units
- Definition of all coordinate frames
- Definition of attitude parameterization (e.g., an Euler angle sequence, quaternion nomenclature, etc.)
- Definition of symbols for the GN&C variables and parameters
  - Mission-specific definitions for terms such as: “ephemeris”, “bandwidth”, “pointing accuracy”, “jitter”, “products of inertia”, “quaternion”, etc.
  - The identification of industry-standard models or databases to be used in analysis and/or simulation (e.g., the JGM3 20x20 gravity model, the Harris Priester atmosphere with solar diurnal bulge, etc.)
- Definition of all time references, conventions and epoch
- Definitions of the GN&C sensor and actuator coordinate frames
- Definition of all mission critical GN&C sensor, actuator or other component alignments
- Definition of all sensor-to-actuator phasing
- Definition of all sign conventions (including definition of signs of products of inertia)
- Error budgets for all GN&C mission modes

Relevant Investigations:

1. What document specifies the set of units and coordinate frames to be used on this project?
2. Are all of the groups that exchange information in inertial coordinate systems using the same True of Date, Mean of Date, or J2000 reference frames?
3. Is the transformation between the different discipline reference frames unambiguously defined in terms of their relative orientation and locations of origin?
4. If dimensionless units are used (e.g. in software) are the normalizing factors identified with their dimensions?
5. What prefixes are permitted for dimensions (e.g. can both centimeters and millimeters be used)?
6. Is there a defined spacecraft time reference, or explicit set of time references, to be used for the mission in question (e.g., UTC, UT1, GPS time, leap seconds, etc)? Have all such time references been documented?

GN&C Best Practice #12

Stringent attention must be paid to stability considerations such as gain and phase margins, damping ratios, and the choice of gain or phase compensation techniques.

Gain and Phase Margins shall meet or exceed 12db and 45 deg at PDR and 6db and 30 deg at CDR. Data latency of commands to actuators contributes phase lag that must be accounted for. A good practice is to assume a latency of one control computational cycle time interval. If the latency is greater than one computational cycle, then round up to the next highest integer of cycles.

Damping Ratios of all flexible body modes shall be assumed to be no greater than 0.1% of critical damping for typical spacecraft (i.e., bolted or pinned joints), unless analysis or test data demonstrate otherwise. However, for those missions where high precision spacecraft/instrument line-of-sight pointing is required, and low amplitude vibrations are critically important, the damping ratio of all flexible body modes shall be assumed to be no greater than 0.05%, unless analysis or test data demonstrate otherwise. In extreme cases, such as ultra-low temperature cryogenic space platforms, the use of a damping ratio in flexible body analyses of greater than 0.01% should be justified with test and/or analysis data.

Gain Stabilization shall be used for control laws and loop compensation of all flexible-body modes, except in special cases where gain-stabilization is shown to be a severe design driver. The peak amplitude of each gain-stabilized flexible-body mode shall not exceed -12 dB in the control system open-loop frequency response. Early in the design phase, the control loop stability analysis should show robustness to variations of +/- 10 % in the lowest frequency modes and +/- 25 % in the highest frequency modes.

Phase Stabilization: Flexible-body modes that do not meet the gain-stabilization requirement above shall have phase margin of at least 60 deg over a modal frequency variation of ±25%, with worst-case time delays included.

Relevant Investigations:

1. Are all time delays and data latency accounted for?
2. Is multi-rate sampling present?
3. Are sensor/actuator pairs collocated?
4. What is the minimum allowable first bending mode frequency of the spacecraft and its appendages?
5. Are any structural mode frequencies within a decade of the controller bandwidth in any control mode?
6. Is there at least +/- 5% separation between flexible mode and the frequency at which actuator commands are issued?
7. How is the structural model initially validated?
8. Is there experimental data for damping ratio over the expected temperature range?
9. Has a rigorous modal significance analysis been used to identify and retain all flexible modes with significant modal amplitudes?
10. How was structural model data integrated into the controller linear model?
11. How are the structural coupling terms used to connect the structural sub-elements?
12. Do the flexible dynamics change over mission?
13. Has the flexible body stability analysis been performed for the full range of deployable appendages?
14. Was the frequency and the amplitude of all flexible modes varied individually or simultaneously?
15. If digital "bending mode" filters (e.g. low pass or notch filters) are used how does execution rate impact the frequency response?
16. Can the filter coefficients and initialization parameters be changed with data uploads instead of SW patches?
17. Are anti-aliasing filters included in the controller?
18. Have Monte Carlo techniques been used to randomize the bending mode frequencies, modal gains, damping ratios, etc. in the stability analyses?
19. How are the stability margins determined in the non-linear time domain simulation? How are they determined in Hardware-in-the-Loop tests?
20. Is structural analysis validated through modal testing?
21. Were there any persistent small amplitude oscillations in closed loop tests or simulations? Were Describing Functions used to study the influence of nonlinearities on stability and the possibility of limit cycles?
22. If the control system has multiple inputs and multiple outputs (MIMO), how were the stability margins determined?

GN&C Best Practice #13

Ensure that the analyses of the dynamics in ALL flight phases are understood completely (e.g. aerodynamics, flexibility, damping, gyrodynamics, plume impingement, moving mechanical assemblies, fluid motion, changes in mass properties, etc.).

Satisfactory dynamic performance of spacecraft ultimately depends upon accurate stability and control analyses. Often sophisticated models of the dynamics of the spacecraft, its control system, and the environment are required in order to perform the required analyses. The first step in planning the analysis and simulation campaign is to identify how precise the models will need to be for the pertinent vehicle dynamics and environments (e.g. aerodynamics, magnetic interactions, flexibility, damping, gyro-dynamics, plume impingement, moving mechanical assemblies, fluid motion, changes in mass properties, etc.). Appropriate planning requires early consultation with dynamics and controls engineers who have broad experience on many missions and detailed experience on the specific types of problems that the current mission might encounter.

During the planning phase, preliminary analysis is required to estimate the magnitude of the environmental disturbances in order to size the control actuators and momentum storage devices appropriately. The disturbance environment may differ by many orders of magnitude over the different phases of a mission. Nevertheless it is usually "paper and pencil" analysis that is needed in the early stages of a program rather than computer simulation. The preliminary analysis is often more critical for systems that seem to be the simplest from a control systems point of view. The dynamics of space vehicles that are stabilized by gravity gradient, spinning, or momentum bias can be highly complex and inappropriate model simplifications such as linearization can lead to unstable designs. Non-linearities and cross-coupling between axes need to be treated with care starting with the preliminary analysis because these phenomena are inherent in the physics; they are not necessarily second order effects that can be added as refinements later. It would be even more dangerous if the detailed performance analysis models used the same simplified assumptions as in a cursory preliminary analysis. Spin stabilized spacecraft often present analytical complications due to energy dissipation, inertia ratio stability constraints, deployment uncertainties, fuel migration and thermally induced asymmetries.

Three-axis stabilized spacecraft with sophisticated attitude determination and control systems may present analytical complications due to non-rigid body dynamics. Prior experience on similar spacecraft usually provides a reasonable basis for estimating how extensive the dynamics analysis and simulation campaign will need to be. Preliminary analysis for three-axis stabilized spacecraft is more likely to be required for unique control system design issues such as controller non-linearities, noise, and timing rather than unknown vehicle dynamics.

Preflight predictions of the performance of GN&C systems are based on simulation because it is so difficult to replicate the space environment in a ground test facility. A Monte Carlo simulation campaign is often used due to the large number of variable parameters (e.g. atmospheric density, gyro noise, thruster valve response times, GPS receiver noise, modal frequencies, damping ratios, etc.) represented in the simulated dynamic model.

Relevant Investigations:

1. Is the system stable over the range of inertias expected?
2. What possible sources of energy dissipation exist? What is the damping time constant?
3. Does the selected GN&C architecture or operational phases, levy inertia ratio constraints on the system (or vice versa)?
4. Are linear control actuators required or will simpler bang-bang control suffice?
5. What is the tradeoff in control system bandwidth between sensor noise and disturbance torque?
6. What sampling rate is required for digital controllers? How much delay is permissible?
7. Is there documentation of the simulation campaign that was used to predict GN&C performance and stability?
8. If the campaign involved Monte Carlo simulation, how many random variables were involved, what distributions for them were assumed, and how was the required number of cases (runs) determined?
9. Describe the process for establishing and validating the model uncertainties.

GN&C Best Practice #14

Make certain that the analyst who develops the math models for the simulation of the GN&C hardware has hands-on familiarity with the hardware being modeled. All unexpected results or anomalies during hardware testing must be explained and/or incorporated into the simulation math model. Similarly all deviations between results from the design simulation and the V & V simulation must be explained.

Skylab, like all space vehicles, was built with careful control of access to keep the vehicle clean, to inventory all material brought inside, and to prevent interference with the assembly and checkout crews. As a result, designers rarely viewed their final product in the as-built condition. Clean room restrictions inhibited the detail designers from examining the hardware, even though several independent reviews had expressed concern about the deployment of the micrometeoroid shield. Consequently the design error that resulted in premature deployment of the shield was not discovered until 63 seconds into ascent when it nearly caused total loss of the mission. An important Lesson Learned was that access to assembly areas should be controlled, but not eliminated.

GN&C systems analysis and simulation studies require detailed models of the guidance and control components (i.e. sensors, electronics, and actuators). The models are developed from component specifications, circuit diagrams, and test results. In the case of sensors and actuators, the models are derived from manufacturer specifications and test results. Models of the electronics are developed by breadboarding and laboratory testing of circuits and components. Test plans and results need to be reviewed by the analyst who develops the model to make certain that the models conform to the hardware as it is actually built. It is highly advisable to have the analyst who develops the math models for the GN&C simulations participate in all the major hardware design reviews as well as witness the hardware acceptance testing and review all test data generated. This will ensure that the analyst has a high level of familiarity with all the idiosyncrasies and behaviors of the GN&C hardware being modeled. The analyst and the test engineer must identify and resolve all test discrepancies. The detection and identification of discrepancies during testing has proved to be crucial to mission success in the past.

The GN&C designers must ensure that they have used adequate dynamic modeling of structural flexibility, plume impingement, outgassing, fuel slosh, nutation, etc. The dynamics and environmental models used in the GN&C design simulations cannot be tested easily in the laboratory. Instead, they are tested against the truth models that were independently derived by the V&V team. The environmental models used in the two simulations can be tested individually by turning off all of the other models of disturbance sources. Similarly, flexible body dynamics can be compared by turning on one flex mode at a time for model validation. In general, the simulation test results will not match perfectly because the models were developed separately, however the sources of the mismatch should be identified. If the mismatch is due to lack of completeness of the design simulation model, then it may need to be modified to provide higher fidelity, which in turn may result in retuning the GN&C system parameters.

Relevant Investigations:

1. Was the analyst who developed the math model of the component present when the hardware test was conducted?
2. Are all the idiosyncrasies and behaviors of the GN&C hardware, for all relevant mission phases, well understood?
3. Was the math model of the component used to predict expected test results? How well did the test results correlate with the expected values?
4. Were discrepancies between test results and expected values due only to parameter variations? Are the parameter variations consistent with the specified tolerances from the component manufacturer?
5. Is the GN&C closed loop system performance sensitive to variations in actuator parameters such as stiction or backlash?
6. Were the physical parameters used in the dynamics and environmental math models based on experimental data? What range of values might be encountered in space during the mission?
7. What are the computational cell size dimensions used in the math models for pressure forces such as aerodynamics and solar radiation pressure? Is shadowing included in the models?

GN&C Best Practice #15

The Truth Model used in Verification of high fidelity simulations must be developed independently from that used in the Design simulation.

Spacecraft contractors have the primary responsibility for performing sufficient stability, control, and dynamics analyses to assure satisfactory dynamic performance of the vehicle. These analyses need to be validated by an independent group in order to assure their completeness and correctness. The formulation of the math models used for verification should be independently derived from those used by the GN&C design engineers. Modeling mistakes are not easily caught. Reusing a model without fully understanding underlying assumptions can be risky. Changes in configuration or flight environment may invalidate the original analysis.

Programs should insist that the analysts document their methodology and assumptions, and compare them against the actual hardware so that errors may be found. Analysis does not negate testing. Component test plans and results must be reviewed to make certain that the models conform to the hardware as it is actually built. Designers should be called back to inspect the products, to see if there are major differences between analysis and implementation.

Polar BEAR (Beacon Experiment and Auroral Research) was a military mission designed to study communications interference caused by solar flares and increased auroral activity. The Polar BEAR spacecraft was gravity-gradient stabilized with an 18.3-m interlocked BISTEM gravity-gradient boom and tip mass, augmented with a constant speed pitch momentum wheel, and a boom-mounted magnetically-anchored eddy-current damper. The spacecraft was built on the Transit-O 17 navigational satellite that was retrieved from the Smithsonian's National Air & Space Museum, where it had been on display for 8 years. It was launched into a near polar orbit on November 14, 1986. For the first few months while the Polar BEAR was in eclipsing orbits, the mission proceeded as designed and its attitude performance was nominal. As it entered its first period of fully sunlit orbit in February 1987, its attitude degraded significantly. The roll, pitch, and yaw angles began oscillating until the satellite finally inverted in May 1987 and stabilized in an upside down attitude.

Previous gravity gradient spacecraft of different design had experienced attitude instabilities but Polar BEAR with its stiffer boom, constant speed wheel and eddy-current damper was expected to be less sensitive to environmental disturbances. However there was no independent truth model to predict Polar BEAR's behavior nor to offer guidance on how to recover from the inversion. Preparations for anomaly recovery should be part of the pre-launch mission planning. Several attempts to re-invert the satellite were undertaken. The third attempt proved to be successful when the momentum wheel was allowed to despin for an orbit before spinning it back to its maximum spin rate. The torque from the wheel in combination with the pitch rate induced from the despinning wheel inverted the satellite and captured it in the desired orientation. Several years later, independent analysis and detailed modeling of the thermal deflection of the boom and coupled system dynamics established that solar heating of the boom was the probable cause of the large-angle attitude motions.

The Polar BEAR anomaly illustrates how unmodelled effects can dramatically perturb a spacecraft's motion. Design changes that were intended to improve the performance of gravity gradient stabilized spacecraft actually introduced unanticipated dynamic interactions that contributed to the on-orbit inversion

Relevant Investigations:

1. If a model has been reused, did the original analyst review the model's applicability for this reuse?
2. Are the physical parameters (e.g. mass properties, gains, deadbands, aerodynamic density etc.) that were used in the design simulations the same as in the verification simulation?
3. How were the math models of the components correlated with H/W test data?
4. Are all of the relevant dynamics modeled (e.g. nutation, multi-body dynamics, relative motion, flexibility, energy dissipation, fluid motion, magnetics, radiation pressure, aerodynamics, changes in moments of inertia due to thermal distortion, eddy current damping, out gassing, impingement, etc.)?
5. Are the simplifying assumptions used in formulating the model (e.g. small angle approximations, linearity, absence of cross coupling, etc.) justified over the entire range of conditions that the model will be used?
6. Has the fault protection logic been independently verified?
7. Does the Truth Model verify that preparations for anomaly recovery are adequate?

GN&C Best Practice #16

Establish a strong relationship with, and maintain close surveillance of, the GN&C lower-tier component-level (both hardware and software) suppliers.

Establishing solid relationships with, and maintaining close surveillance of, the GN&C hardware and software component suppliers is a Best Practice for both human rated spacecraft and robotic spacecraft developments. However, one would expect that the level of GN&C supplier surveillance would be substantially higher when procuring components for human rated spacecraft versus robotic spacecraft.

The Apollo Program placed an extraordinary emphasis on GN&C component reliability. It was a single-string system with no redundant features, and thus, no fault tolerance. To achieve this unprecedented level of component reliability, a set of extremely rigid and comprehensive quality control processes were developed and applied by NASA on all GN&C parts and components suppliers. To satisfy the need for an ultra-reliable GN&C system, some industrial contractors established special NASA-dedicated production lines, using NASA certified trained assemblers. NASA continuously performed on-site inspections of the GN&C component production lines at selected industrial contractors. At the electronic device level, devices were tested and if a single sample proved defective the entire device lot was quarantined. Failed devices went through detailed teardown and failure analysis to preclude defect migration problems.

Following Apollo, NASA purposefully moved away from a single-string GN&C architectural approach for its human rated spacecraft. Having fault tolerant spacecraft GN&C systems, however, does not mean that NASA has the luxury of relaxing requirements for GN&C component-level reliability. It is expected that the prime industrial contractors of the CxP spacecraft will have the leadership role in procuring GN&C components for their respective vehicles from the lower-tier suppliers. It would be inappropriate, unwise, and complacent for NASA to relinquish to the industry primes the entire responsibility for monitoring and overseeing the component development and production work at the suppliers.

Relevant Investigations:

1. What is the component/supplier selection process and what criteria are used?
2. Was selection based on lowest cost to just meet the minimum technical requirements?
3. Can performance be improved with modest cost?
4. What is the past-performance of the suppliers?
5. How are parts, materials, and processes for a Human rated program qualified and verified?
6. What Mission Assurance requirements are placed on GN&C suppliers and how are they enforced?
7. Are there incentives for meeting performance or cost and schedule goals?
8. Are there any limitations on government's access to suppliers particularly for test witnessing?
9. What are the component test philosophies, criteria and implementation to detect/screen out material, part, fabrication process, workmanship, and assembly defects in each component?
10. Is the workforce of proper size and skill mix?
11. How are test discrepancies and anomalies reported, tracked and resolved?
12. Are all test facilities in-house or are some outside?
13. Does prime intend to co-locate engineering and mission assurance staff at the supplier?
14. How well has the supplier applied lessons learned to his own DDT&E processes?
15. Are all technologies mature?
16. Which components qualify by similarity?
17. Which components require re-qualification?
18. Are sensors analyzed for worst-case signal-to-noise degradations?
19. Does testing protect flight hardware personnel?
20. Will an Engineering model be used as a "pathfinder"?
21. How will the Initial Power-on Test (IPT) protection be validated?
22. Are there any special test fixtures or equipment not yet identified?
23. Will Thermal/Vacuum testing in addition to ambient-pressure thermal cycling be performed?
24. Where will component life testing be performed?
25. If accelerated life testing is planned how is it justified? Are the failure mechanisms identical in an accelerated life test?
26. Does the supplier intend to perform any tests for "discovery"? If so, what is the justification or rationale for such tests?
27. How will documentation be controlled and maintained for traceability of parts, materials, processes and testing on each flight component?
28. How are qualification and acceptance levels set?

GN&C Best Practice #17

The GN&C subsystem should adhere to the "Test As You Fly" philosophy.

In the Verification and Validation (V&V) phase, GN&C Engineers should "Test As You Fly; Fly as you test". "Verification" shows that the system satisfies the design requirements whereas the "Validation" demonstrates that the system actually performs as intended.

It is difficult to "Test GN&C systems As You Fly", due to the 1-g ground test environment. GN&C V&V therefore relies upon analysis, simulation, inspection, and demonstration. When analyses and/or simulations are used, results need to be independently reviewed. When inspections are used, they must be performed on the final, as-built, ready-to-fly GN&C configuration.

GN&C Flight Software must undergo closed-loop validation running on the same platform as the GN&C host computer. It must be tested with nominal, failed and degraded GN&C components, over the full range of mission profiles, flight dynamics, and spacecraft models. If the flight computer on the Ariane 5 Flight 501 mission had been tested with the Ariane-5 trajectory, rather than the Ariane-4 trajectory, the flaw in the software code that resulted in the loss of the mission would probably have been discovered before flight.

Some GN&C functions can be tested on the ground without going to extraordinary measures. End-to-End attitude controller polarity tests can be performed in a relatively straightforward manner for example. These types of tests, however, must be performed with rigorous knowledge and control of the test configuration. All such tests should be performed in the actual flight configuration, including the flight electrical harnesses and final GN&C flight software builds.

Expected test results should be established and documented well in advance of the actual test execution. The expected GN&C test results should be reviewed and understood by the test team prior to performing that test. GN&C testing is to be performed for the purposes of verification, not for "discovery".

Relevant Investigations:

1. How will GN&C stability and performance be verified in various configurations prior to flight?
2. Does the test plan specify all test activities, roles, responsibilities, methods, facilities and venues, models, support equipment, and schedule?
3. What are the minimum tests to be completed prior to launch? How are deviations to be handled?
4. Are there GN&C tests that can be performed on the ground but will not? Why?
5. Are GN&C testing limitations and uncertainties defined, documented and included in risks?
6. Will actual GN&C flight hardware or non-flight engineering units be used in tests?
7. How is "Test As You Fly" applied to GN&C testing?
8. Are exceptions to "Test-As-You-Fly" identified and documented with risk assessment?
9. Is GN&C end-to-end (sensor to actuator) controller polarity testing performed in the flight configuration?
10. Will simulated on-orbit "day in the life" operation of the GN&C subsystem be performed under nominal and stressed conditions for all mission critical events?
11. Which tests are performed in thermal/vac or vibration environments?
12. How will test configurations be maintained and controlled? What configuration management steps are used to control GN&C hardware and software interfaces for GN&C testing?
13. Does testing require unique procedures, Special Test Equipment, GSE, facilities or training?
14. Are expected results defined before actual tests?
15. Will an independent GN&C engineer certify tests plans as adequate for GN&C verification?
16. Will the same Cmd/Telemetry system that will be used for Flight Operations also be used for test?
17. Is the same GN&C Trend database used for key component functional and performance metrics during ground test and on-orbit?
18. What integrated spacecraft testing can be done prior to launch processing? What are the test limitations? What testing can be performed on the launch pad?
19. What is retested if the tested flight ready GN&C configuration is altered?
20. When is the last opportunity to ensure the GN&C subsystem will perform?
21. Are test flights planned to fill gaps in ground tests?
22. Are there on-orbit tests that must pass prior to proceeding to the next mission phase?
23. Have the GN&C FSW maintenance procedures, including realtime code patches, been demonstrated using flight-like communications links?

Best Practice #18

Conduct true End-to-End Sensors-to-Actuators Polarity Tests in all flight hardware/software configurations, including all flight harnesses/data paths. Resolve all test anomalies.

Spacecraft use many GN&C components that can be easily reversed during installation. There have been many serious on-orbit problems, some leading to total mission failure, due to inadequate verification of signal phasing or polarity. Both component-level and end-to-end phasing tests are necessary to ensure correct operation. All GN&C sensors and actuators must undergo end-to-end phasing/polarity testing after spacecraft integration. The tests must be conducted using the same physical configuration and operational modes used in flight.

The Thermosphere, Ionosphere, Mesosphere, Energetics and Dynamics (TIMED) spacecraft is a 600 kg spacecraft that employs a three-axis zero-momentum Attitude Control Subsystem (ACS). Following launch on 12/07/2001 there were several anomalies in the GN&C system. The first ACS problem encountered was a sign error in the magnetic torque rod control logic used to unload accumulated angular momentum in the reaction wheels. This polarity error occurred because well established protocols for End-to-End Polarity tests prior to launch were not followed. Fortunately, the ground operations team had nearly continuous, early on-orbit realtime command and telemetry contact with the spacecraft via TDRSS which allowed them to observe and then quickly correct this potentiality dangerous ACS sign error (See Best Practice #21).

The second ACS problem encountered on TIMED was that the spacecraft attempted to point the wrong axis towards the Sun. Fortunately one of the solar arrays was still illuminated in this unplanned orientation so the spacecraft remained power positive while the anomaly was diagnosed. I&T photographs of the Sun sensors revealed that two of the four Sun sensors were mounted ninety degrees away from what was intended. The root cause of this problem was that the polarity tests during the spacecraft I&T had not been performed with the satellite in its actual flight configuration. The two sun sensors were mounted to a panel through which the internal access to the spacecraft was attained during I&T operations. The panel was removed and was not in its flight configuration during most of the I&T activity. The two Sun sensors were temporarily hung off to the side. Unbeknownst to the ACS team, the orientation in which they were hung did not agree with the orientation they would have in flight. The "Test as You Fly" engineering best practice had not been adhered to in this case (See Best Practice #17).

An example of a mission failure due to incomplete End-to End testing is the Tomographic Experiment using Radiative Recombinative Ionospheric Extreme ultraviolet and Radio Sources (TERRIERS) satellite. Following launch on May 18, 1999 ground controllers observed the spacecraft losing power and determined that the spacecraft was not able to orient itself properly to allow its solar panels to fully face the Sun. Telemetry data indicated that the spacecraft was in the correct orbit and was spinning appropriately about the right axis. The subsequent failure investigation determined the cause of the TERRIERS failure was an ACS polarity error that had the effect of off-pointing the spacecraft's solar array by 180 degrees. Complete mission failure was therefore due to inadequate end-to-end attitude control system polarity testing in the flight configuration.

The scientific goal of the Genesis Sample Return mission was to collect pristine material from the solar wind and return these samples to Earth. During reentry, the parachute system failed to deploy because the gravity-switch sensors were reversed in orientation. The spacecraft's verification process did not detect the gravity-switch design error because there was a failure to adhere to the 'Test as You Fly' approach to space system testing.

Relevant Investigations:

1. Do photographs show that sensors and actuators are mounted in the same positions and orientations (S/C coordinate frame) during polarity tests as they will be in flight?
2. Is the potential reorientation of the GN&C sensors due to on-orbit appendage deployments properly taken into account?
3. Were any special non-flight test cables or data paths used in the ground tests?
4. Were tests conducted in all GN&C operating modes that will be used in flight? Were all switches and/or relays properly accounted for?
5. Did the test plan detail the expected results? Were all deviations between expected and actual test results accounted for?
6. Were modifications made to equipment or procedures as a result of the test? Were tests then repeated?
7. Does the flight software code or database allow easy (e.g., simple data table updates) correction of any latent GN&C polarity problems that are discovered during early on-orbit operations?

Best Practice #19

Conduct sufficient GN&C Hardware-in-the-Loop testing to verify proper/expected HW/SW interactions in all operational modes, during mode transitions and all mission critical events.

The hand-over of the GN&C system functions, such as when mode switches occur in flight software or when sensor or actuator hardware is swapped, must be done in a definitive and non-disruptive manner. The initialization and termination of attitude controllers and navigation filters must be unambiguous and result in graceful transitions between states. It may be desired to use the information about the end states of one GN&C system configuration as inputs for the initial states of the new configuration. The hand-over must be crisply enabled such that the new configuration is completely in charge and the former configuration has no further effect. Conflict between control configurations can result in loss of control. All hand-overs of the GN&C system functions must be tested in the flight configuration of the H/W and S/W to verify that the transitions are free of undesirable transients and perturbations.

The Mars Polar Lander (MPL) mission failure is illustrative of the need for rigorous GN&C Hardware-in-the-Loop testing to verify proper end-to-end operation during mode transitions and all mission critical events. The mission objective of the MPL was to soft land near the South Pole of Mars. The communications with the spacecraft ceased, as planned, at the start of atmospheric entry and nothing more was ever heard from the lander. The failure investigation board concluded that the most likely failure mode was that the lander's GN&C system (which controlled the firing of the RCS engines used to decelerate the vehicle to a soft landing) would interpret the vibrations as the lander's legs were deployed as an indication of surface contact and then consequently shut down RCS engines too early causing the vehicle to crash to the surface. It was believed that a software error in how data/signal from Touchdown sensor on lander legs was used. It was noted that an end-to-end test of the landing system was deleted from the MPL test sequence due to schedule pressures. MPL was therefore a complete mission loss.

Clementine is another case where inadequate testing of end-to-end system operation during a computationally stressful mission critical event led to mission termination. A fatal GN&C/flight software interaction occurred shortly after the start of a propulsive maneuver. A malfunction in the on-board computer controlling the thrusters used up all of its fuel, leaving the spacecraft spinning at about 80 RPM with no spin control. The simultaneous increase in computational burden to control the thruster firings along with an unanticipated numeric overflow caused the flight computer to "freeze" resulting in an uncontrollable spacecraft spin-up. There was a watchdog timer intended to inhibit continuous thruster firings but it did not function because the computer had crashed. One can presume that this vulnerability would have been revealed had complete end-to-end "stress" testing of this mission critical event been performed. Note that the Clementine spacecraft was designed and developed using an acquisition and management philosophy very similar to NASA's "Faster, Better, Cheaper" (FBC) approach.

Relevant Investigations:

1. Does the design rigorously control configuration, especially at hardware/software interfaces? Can glitches propagate across interfaces?
2. Were flight-critical functions tested with flight cables and data system hardware in the loop?
3. Does test plan include nominal and anomalous operational scenarios? Are all credible failure paths (e.g. part transients, latch-up, over-voltage, and EMI) included?
4. Did tests include realistic switching between redundant components and/or controllers?
5. Are there test points or S/W in the design that are used only during test? How are they disabled for flight?
6. Have non-flight Engineering Units (EUs) been used to support GN&C HITL testing?
7. What is the cost/benefit analysis of using flight units vs. EUs? Has the risk of damaging flight hardware during HITL testing been assessed?
8. How will configuration control between flight and test units be managed?
9. How will GN&C idiosyncrasies found during HITL testing be addressed, documented and provided to the design team, ground ops team and flight ops team?
10. Are there off-nominal HITL test cases to rigorously stress the integrated GN&C system in anomalous and contingency scenarios?

Best Practice #20

Treat GN&C ground databases, uploads, ground application tools, command scripts/files etc. with the same disciplined care that the GN&C Flight Software code and data are treated.

Engineers who initially conceive and design a GN&C system often do not remain with the program through its entire life. Consequently, the rationale for selection of certain parameters or procedures may not be apparent to spacecraft operators at a later time. Ad hoc changes in the databases or procedures can cause operational errors that may be fatal to the mission. Thorough training and adherence to the established procedures for ground software/database configuration management, documenting change history, version archiving, and peer review is essential for the flight operations team. The Relay Mirror Experiment (RME) provides an example of the need for ground operators to understand the GN&C flight software well enough so that the flight and ground databases can be made compatible. RME started tumbling immediately after launch when attitude determination failed and the momentum wheel was shut off. The ACS shut off because an ephemeris file used in ground test had been left in the flight computer. When a proper ephemeris file was uploaded to the spacecraft, attitude control was restored and the mission went on to success.

Procedural errors by the SOlar Heliospheric Observatory (SOHO) spacecraft's Flight Operations Team (FOT) caused the vehicle to suffer a major "loss of attitude" anomaly in June of 1998 (Reference 4). This anomaly occurred during a planned period of calibrations, maneuvers, and spacecraft reconfigurations. Prior to this anomaly the SOHO FOT had concluded two years of successful science operations. Many SOHO operational procedures, such as those for momentum management, gyro calibration, and science instrument calibration, had been successfully executed over that two-year period. These "housekeeping" procedures were typically grouped together by the flight operations team to minimize the impact on SOHO science downtime. Prior to the anomaly these procedural groups had been executed in discrete blocks over the course of a single twelve-hour operations team shift. This well-established and flight-proven procedural practice was modified just prior to the anomaly. These procedural modifications were part of a larger SOHO operations re-engineering activity intended to reduce operations cost for the SOHO extended mission, to streamline the operations to minimize science downtime, and to conserve gyro life. Specifically the operation had been compressed into a continuous procedural sequence, which required a new command script and first time utilization of paths within modified procedures. The anomaly was, in part, due to an omission in the modified command sequence. This omission resulted in disabling the normal spacecraft Safe Hold Mode functionality. A gyro needed for proper Safe Hold Mode attitude control was not enabled due to the omitted command. A second error in another predefined command sequence caused another gyro, whose output signal was used in on-board fault detection, to be erroneously left in its high gain setting. This error resulted in a gyro-indicated spacecraft roll rate of twenty times greater than the actual rate. As a consequence the on-board fault detection logic placing the SOHO spacecraft into a Safe Hold Mode, a five-hour spacecraft emergency situation ensued during which the SOHO FOT formulated an incorrect diagnosis of the on-orbit state of the spacecraft. Their subsequent response (based upon the faulty diagnosis) resulted in loss of the vehicle's attitude control, followed by loss of command/telemetry communications contact, and then loss of power and thermal control. The joint ESA/NASA mishap investigation board concluded that this SOHO incident was a direct result of operational errors, a failure to adequately monitor spacecraft status, and an erroneous decision which disabled part of the on-board autonomous failure detection. Further, following the occurrence of the emergency situation, the board found that insufficient time was taken by the operations team to fully assess the spacecraft status prior to initiating recovery operations. The board recommended that a comprehensive review of SOHO flight operations be conducted addressing issues in ground procedures, procedure implementation, management structure and process, and ground systems.

Relevant Investigations:

1. Are command scripts formally controlled?
2. How are yellow caution and red alarm telemetry limits set? Is there an independent analysis of the limit values before flight?
3. What is the process to change the databases?
4. Is the I&T GN&C Command and Telemetry system the same as used for Flight Operations?
5. Under what operational circumstances must a GN&C system design engineer be notified?
6. What type and extent of GN&C training is provided to the flight operations team?
7. Does the GN&C documentation detail the rationale for ACS parameters and ops procedures?

Best Practice #21

Ensure that sufficient GN&C engineering telemetry is down-linked, processed, and made available to diagnose anomalies, during all mission phases including early on-orbit operations when many failures occur.

Anomalies occur in even the best of systems. The most important factor in resolving them is getting the right telemetry data. Having good data greatly simplifies and speeds diagnosis of the root cause of the anomaly. Routine telemetry for evaluating normal operations is often inadequate to help resolve anomalies efficiently. Good diagnostic data includes many more variables and is sampled at a significantly higher rate. Plans for diagnostic telemetry should be included in the initial designs of the GN&C and telemetry systems. It is advisable to develop ground displays for GN&C engineers working launch and mission operations that enable quick identification and diagnosis of problems. A dedicated real-time GN&C simulator allows realistic training and rehearsal of these critical GN&C operations.

The Sun pointing ACRIMSat is spin stabilized about its major axis of inertia. After injection into low Earth orbit the spacecraft spun up to 12 rpm using magnetic torquers. Spin rate sensing and commutation of the magnetic torquers was derived from a three-axis magnetometer. The only other sensors on-board were two types of sun sensors to control precession and an accelerometer to measure nutation. As the spin rate increased the angle to the sun started to increase rather than decrease. It was apparent from the limited telemetry that was available in the first few ground contacts following the launch that at least one control loop was unstable. Coarse control was regained following the command to switch to Sun sensor nutation damping. This was a quick fix that saved the mission but several weeks would pass before thorough processing of the telemetry would reveal what had gone wrong. ACRIMSat was a product of the "Faster, Better, Cheaper" (FBC) approach. Unfortunately this resulted in incomplete planning for contingency operations. The ground software needed to process attitude telemetry was not in place to support the early orbit anomalies.

It was postulated that ACRIM's accelerometer based nutation control loop was the source of the initial divergence from Sun pointing. In order to prove this, it was necessary to show that the initial telemetry data was consistent with an instability that would result from a single sign error in the accelerometer based nutation control loop. The isolation and correction of the suspected sign error was difficult due to the limited data types (3-axis magnetometer, 2-axis sun sensor, and 1-axis accelerometer) and intermittent telemetry downlinks due to widely separated ground contacts. The sun sensor and magnetometer data was processed with a TRIAD algorithm to obtain inertial body attitude as a time-function. This was then transformed into body rates and then Fourier filtered to show the body rate component at nutation frequency. Similarly, the accelerometer data was Fourier filtered to isolate the nutation frequency component. The accelerometer output was correctly phased to measure the X-axis rate due to nutation, despite any uncertainty that might have existed about its correct polarity at the time of its installation on the spacecraft. The sign reversal was therefore in the control algorithm and was corrected with a software patch.

One should also note that a contributing factor to the LEWIS spacecraft failure was the fact that the GN&C telemetry was not monitored during the critical 12-hour period following launch.

Relevant Investigations:

1. Are there plans to add the on-orbit trend data to the GN&C performance trend database built during I&T?
2. How many telemetry variables are available for normal operations and diagnostics? How many spare data slots exist?
3. What are the sample rates for normal engineering data and diagnostic data?
4. What is the maximum angular velocity during a worst-case anomaly? Is the diagnostic data rate high enough, and data scaling appropriate, to unambiguously track the relevant parameters in that situation?
5. Is diagnostic data automatically buffered or does it require a command? How much diagnostic data can be stored on-board?
6. Can telemetry capture non-routine GN&C engineering data in support of anomaly resolution?
7. Can new GN&C telemetry points be added on-orbit in a high data rate "dwell mode" manner, including re-scaling selected telemetry?
8. Is ground software available to process attitude telemetry in support of contingency operations?
9. Do the operations plans include around the clock monitoring of telemetry during early orbit and mission critical events?

Best Practice #22

"Train as They Fly": Use a dedicated real-time GN&C simulator facility to realistically train and rehearse GN&C operations in the manner that they expect to actually fly the spacecraft.

Flight simulators are increasingly critical elements in astronaut training and requirements analysis. Simulator fidelity must meet escalating demands in crew training requirements. The simulators must be changed to match the cabin layout of each individual spacecraft, and should provide the crew with all the sights, sounds, and movements they would encounter in actual flight. The flight simulator can also be used to validate GN&C command/telemetry data flows between the spacecraft and the ground network. It can be also used to support on-orbit operations, especially to checkout and validate new GN&C contingency procedures. The ability to implement alternate operational procedures and tests proved life saving in Apollo 13.

Flight simulators with realistic GN&C attributes will be vital in future astronaut training. Astronaut "hands-on" involvement in the design and development of the GN&C systems and associated flight simulators is a must. Intensive training in a realtime functional simulator, not only trains the crew in GN&C operations, but also permits crew feedback that enhances safety, efficiency, and mission success. Realistic astronaut training will help define critical displays/controls, mode sequencing, intervention provisions, and alternative procedures and abort.

The use of high-fidelity flight-like simulators for training astronauts can be traced back to the mid-1960s during the Apollo Program. The Apollo astronauts relied much more heavily on spacecraft simulators than did the Gemini crews. Several key factors emerged during the Apollo Program as critical for flight simulators. First among these was the need for high-fidelity crew stations, especially for GN&C controls and displays. Another was the accurate simulation of the guidance computer and navigation systems. Others included complete visual display of out-the-window scenes and moving-base simulators for high-fidelity training in particular phases of the missions. To meet these needs the MIT Instrumentation Laboratory developed a hybrid analog-digital simulation of the Apollo GN&C System. This simulator was initially conceived of as an alternative validation tool for certain of the on-board GN&C computer programs written by MIT. The hybrid simulator complemented the all-digital simulation, which contained a bit-for-bit simulation of the Apollo Guidance Computer (AGC), which was used as the primary verification tool for the on-board GN&C programs. The hybrid Apollo simulation facility offered certain advantages over the all-digital simulation; it operated in real time and allowed manual access to the AGC during the simulation, as well as on-line monitoring of the progress of the simulation. Subsequently, the simulator was enlarged to incorporate a partial Command Module cockpit mockup containing displays and controls. This version of the simulator proved extremely valuable for testing the man-machine interface with the on-board computer programs and was used for essential GN&C familiarization training of the Apollo flight crews. Switches and controls were designed to have exactly the same "feel" as flight articles and produced responses exactly like those that would be generated during a mission. This allowed the astronauts to practice inputting manual commands to the AGC for mode control, attitude and translation control, etc. The cockpit mockup also contained flight-like optical hardware, along with simulated star field data, permitting the crew to practice, in a safe ground environment, the navigational techniques they would need in space for updating the alignment of their IMU via stellar sightings.

Also note that the Shuttle program includes a Shuttle Avionics Integration Laboratory (SAIL) and Shuttle Motion Simulator (SMS) facility with real time operation and cockpit set-up. The SMS is used primarily for training and the SAIL is an engineering simulation that is open to Astronaut participation.

Relevant Investigations:

1. Does the contractor intend to develop a realtime spacecraft simulator, especially for GN&C familiarization training? If so, how many will there be and where will they be located?
2. Are there special GN&C crew training requirements/needs? How will they be satisfied?
3. What will be the fidelity of the GN&C subsystem emulation in such a simulator?
4. What range of situations (nominal and off-nominal) was tested with crew in the loop to ensure the design was robust?
5. Have GN&C contingency procedures been developed using the flight simulators exercising all aspects of the critical mission phases?
6. Based on simulator testing, what information is deemed essential to the crew's realtime understanding of the state of the vehicle(s)?
7. What information is deemed essential to crew's understanding of the state of the automation?
8. Have the GN&C displays and control mechanisms (e.g., hand controllers, keyboards, etc) been refined via use of the simulator?

Acknowledgments

The results presented in this paper were produced with the support of several individuals from various organizations. The authors would like to thank and acknowledge the significant technical contributions of the following individuals: James Blue, Michael Cleary, Jerold Gilmore, Bruce Jackson, Scott Miller, and Dorre Poppe. The members of the NESC Leadership Team at NASA's Langley Research Center are also acknowledged for their support and encouragement of the work of the GN&C TDT in developing the Best Practices described in this paper. James Miller and Christina Cooper at NASA/LaRC are acknowledged for their assistance in editing and refining our NESC GN&C Best Practices final report. Lastly, the authors gratefully thank Dr. Jesse Leitner of NASA/GSFC for his thoughtful review of and commentary on this paper.

References

[1] **"**The NASA Engineering & Safety Center (NESC) GN&C Technical Discipline Team (TDT): Its Purpose, Practices and Experiences", C. J, Dennehy, AIAA-2007-6332, GN&C Annual Conference, Hilton Head, SC, August 2007

[2] "Design, Development, Test & Evaluation (DDT&E) Considerations for Safe and Reliable Human Rated Spacecraft Systems", NASA Engineering and Safety Center Report RP-06-108/05-173-E, Volume 1 (Spacecraft Systems Engineering with a Safety and Reliability Focus) and Volume 2 (Spacecraft Subsystems), May 2007

[3] "Summary Overview of the DART Mishap Investigation Results, Public Release Version, 15 May 2006.

[4] "SOHO Mission Interruption Joint NASA/ESA Investigation Board Final Report", NASA/ESA Document, 31 August 1998

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-01-2008	Technical Memorandum	August 2007

4. TITLE AND SUBTITLE

GN&C Engineering Best Practices For Human-Rated Spacecraft Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dennehy, Corneilus J., Lebsock, Kenneth; and West, John

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

510505.06.07.03.99

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

NASA Engineering and Safety Center
Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER

L-19446

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITOR'S ACRONYM(S)

NASA

11. SPONSORING/MONITORING REPORT NUMBER

NASA/TM-2008-215106

12. DISTRIBUTION/AVAILABILITY STATEMENT

Publicly Available Availability: NASA CASI (301) 621-0390
Subject Category 18 - Spacecraft Design, Testing and Performance

13. SUPPLEMENTARY NOTES

AIAA Guidance, Navigation and Control Conference and Exhibit AIAA 2007-6336 20-23 August 2007, Hilton Head, SC

14. ABSTRACT

The NASA Engineering and Safety Center (NESC) recently completed an in-depth assessment to identify a comprehensive set of engineering considerations for the Design, Development, Test and Evaluation (DDT&E) of safe and reliable human-rated spacecraft systems. Reliability subject matter experts, discipline experts, and systems engineering experts were brought together to synthesize the current "best practices" both at the spacecraft system and subsystems levels. The objective of this paper is to summarize, for the larger Community of Practice, the initial set of Guidance, Navigation and Control (GN&C) engineering Best Practices as identified by this NESC assessment process.

15. SUBJECT TERMS

NESC, GN&C, DDT&E, spacecraft, reliability

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
UU	UU	UU	UU	31	19b. TELEPHONE NUMBER *(Include area code)* (301) 621-0390